

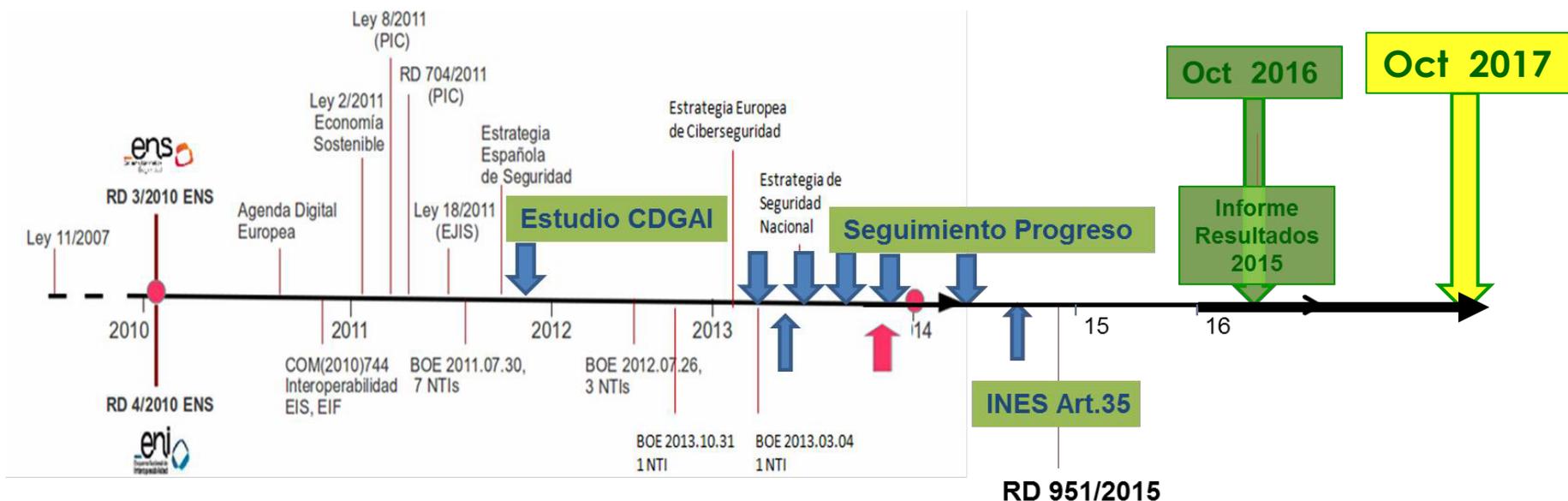


GENTRO GRIPTOLÓGICO NACIONAL

# INFORME NACIONAL DE SEGURIDAD PARTICIPACIÓN 2017 RESULTADOS INES 2016 ENTIDADES LOCALES



## INES - CAMPAÑA 2017



Ya venció el plazo de 48 meses para la adecuación al ENS (RD 3/2010)

El RD 951/2015 añade 24 meses al plazo inicial



Noviembre 2017

Ley 39 y 40 amplía ámbito del ENS

## ESQUEMA NACIONAL DE SEGURIDAD



## Principios básicos

- a) Seguridad integral
- b) Gestión de riesgos
- c) Prevención, reacción y recuperación
- d) Líneas de defensa
- e) Reevaluación periódica
- f) La seguridad como función diferenciada

6



## Requisitos mínimos:

- a) Organización e implantación del proceso de seguridad.
- b) Análisis y gestión de los riesgos.
- c) Gestión de personal.
- d) Profesionalidad.
- e) Autorización y control de los accesos.
- f) Protección de las instalaciones.
- g) Adquisición de productos.
- h) Seguridad por defecto.
- i) Integridad y actualización del sistema.
- j) Protección de la información almacenada y en tránsito.
- k) Prevención ante otros sistemas de información interconectados.
- l) Registro de actividad.
- m) Incidentes de seguridad.
- n) Continuidad de la actividad.
- o) Mejora continua del proceso de seguridad.

15



## Medidas de seguridad

(Protección adecuada de la información)

- a) Marco organizativo.
- b) Marco operacional.
- c) Medidas de protección.

75

1. Los **Principios básicos**, que sirven de guía.
2. Los **Requisitos mínimos**, de obligado cumplimiento.
3. La **Categorización de los sistemas** para la adopción de **medidas de seguridad** proporcionadas.
4. La **auditoría de la seguridad** que verifique el cumplimiento del ENS.
5. La **respuesta a incidentes de seguridad**. Papel de CCN- CERT.
6. El uso de **productos certificados**. A considerar al adquirir los productos de seguridad. Papel del Organismo de Certificación (CCN).
7. La **formación y concienciación**.



# ÍNDICE

1. Herramienta INES
2. Participación (2017)
3. Categorización de Sistemas
4. Resultados
5. Conclusiones y próximos pasos



# ÍNDICE

1. Herramienta INES
2. Participación
3. Categorización de Sistemas
4. Resultados
5. Conclusiones y próximos pasos

### 3. Artículo 35 RD 951/2015 : ESTADO DE SEGURIDAD DE LAS AAPP

El **Comité Sectorial de Administración Electrónica** articulará los **procedimientos** necesarios para **conocer** regularmente el estado de las principales **variables de la seguridad** en los sistemas de información a los que se refiere el presente real decreto, de forma que permita elaborar un perfil general del estado de la seguridad en las Administraciones públicas.

El **Centro Criptológico Nacional** articulará los procedimientos necesarios para la **recogida y consolidación de la información**, así como los aspectos metodológicos para **su tratamiento y explotación**, a través de los correspondientes grupos de trabajo que se constituyan al efecto en el Comité Sectorial de Administración Electrónica y en la Comisión de Estrategia TIC para la Administración General del Estado.

# INFORME NACIONAL ESTADO SEGURIDAD



- CCN-STIC 815 Métricas e Indicadores
- CCN-STIC 824 – Información del Estado de Seguridad
- CCN-STIC 844 - Manual de usuario de INES

## Organismos bajo el alcance del Esquema Nacional de Seguridad (ENS)



AGE



CC.AA.



EE.LL.



Universidades

[www.ccn-cert.cni.es](http://www.ccn-cert.cni.es)  
Acceso INES

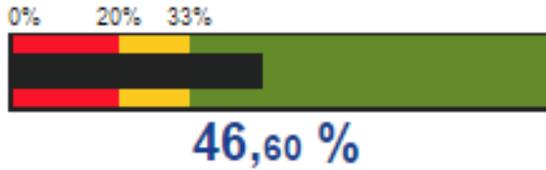


Registro de Información de Seguridad



Resultados: Indicadores de madurez y cumplimiento

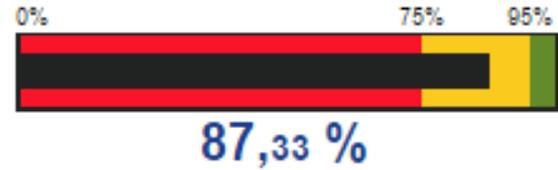
INDICADOR DE MADUREZ DEL ENS  
(index.maturity.ens)



Mediana para AGE con sistemas de categoría Básica: 42,73 %  
Mediana para AGE: 56,00 %

[Pulse aquí para ver la información necesaria para calcular este indicador](#)

INDICADOR DE CUMPLIMIENTO DEL ENS  
(index.compliance.ens)

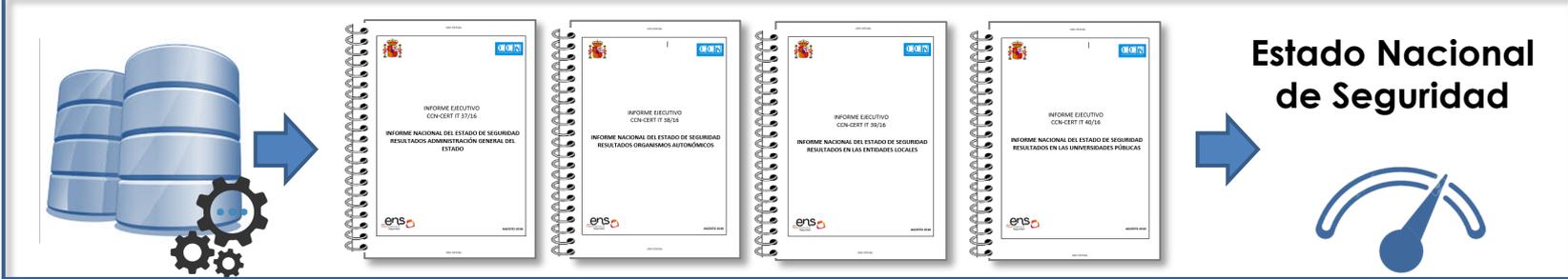


Mediana para AGE con sistemas de categoría Básica: 57,07 %  
Mediana para AGE: 70,24 %

[Pulse aquí para ver la información necesaria para calcular este indicador](#)



Resultados: Generación de informes agregados



## INES - ACCESO

- Registro portal CCN-CERT
- Acceso a INES

The screenshot displays the CCN-CERT portal interface. At the top, the header includes the CCN-CERT logo and the text "DEFENSA FRENTE A LAS CIBERAMENAZAS". A navigation bar contains links for Inicio, Sobre nosotros, Gestión de incidentes, Formación, Guías, Informes, Herramientas, ENS, Empresas, Seguridad al día, and Registro. Below the navigation bar, there is a "ÚLTIMA HORA" section with a news item: "Apple publica la lista de las 25 aplicaciones afectadas por el malware". To the right, a "NIVEL DE ALERTA" indicator shows "MUY ALTO" with a red bar. The main content area features a central dashboard with a globe and various data visualizations. On the right side, there are four blue buttons labeled SAT, CURSOS ONLINE, ENS, and INCIDENTES. At the bottom, a horizontal toolbar contains five icons with labels: CARMEN (Herramienta de Detección de APTs), CCNDroid (Herramientas de Seguridad para Android), CLARA (Auditoría de Cumplimiento ENS/STIC en Sistemas Windows), INES (Informe de estado de Seguridad en el ENS), and LUCIA (Sistema de Gestión Federada de Tickets). The INES icon and the "Herramientas" menu item are circled in red.



# INES – RELACIÓN CON OTRAS HERRAMIENTAS

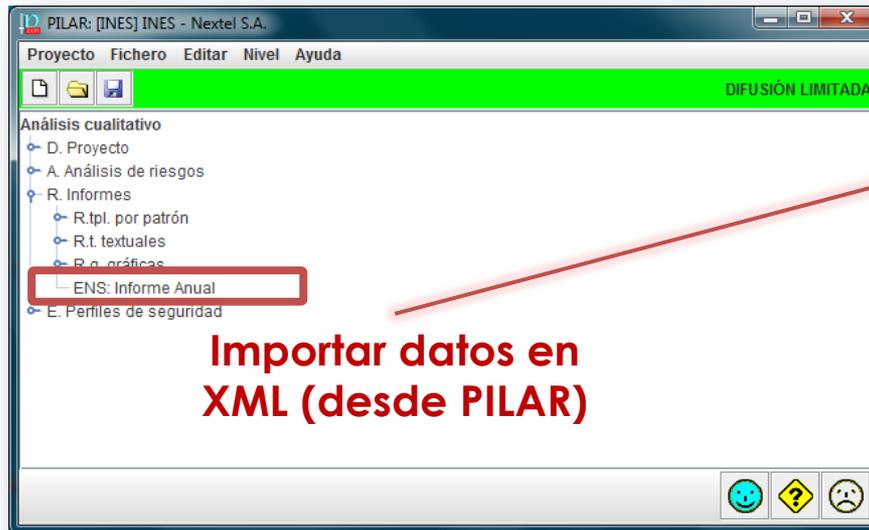


Herramientas de análisis y gestión de riesgos.



Informe del Estado de la Seguridad en el ENS.

**PILAR permite exportar datos en XML en el formato requerido por INES**



## INES – OUTPUT



## INES – OUTPUT

1

## INFORME GLOBAL INES

<input type="checkbox"/> Todos	TITULO	DESCRIPCIÓN
<input type="checkbox"/>	Informe global INES 2016	Listado de todos los datos de 2016
<input type="checkbox"/>	Informe global INES 2015	Listado de todos los datos de 2015
<input type="checkbox"/>	Informe global INES 2014	Saca un listado de las entidades con todos sus datos

«« Página 1 de 1 »» 20 Registros por página

## SELECCIONE LAS FICHAS A VOLCAR

Plantilla:	2016 seguimiento estado ENS ▼
Ficha:	2016 AENA ▼
Protegido con contraseña:	<input type="checkbox"/>
Nombre del fichero de volcado:	<input type="text"/>

# INES – OUTPUT

2



## INFORME INDIVIDUAL DE RESULTADOS

Plantilla: 2016 seguimiento estado ENS



Usuarios con acceso: 14

Validaciones pendientes: 0

Nivel de validado y rellenado:



V: 93.56% R: 93.56%



[Ver el cuadro de mandos](#)

[Generar informe de resultados](#)

Pincha aquí para importar los datos desde un XML.

**INFORME GLOBAL ESTADO DE SEGURIDAD**  
CIEMAT  
2016

**1. METODOLOGÍA**  
Este informe de datos es la respuesta a la herramienta del Estado de Seguridad basadas en la metodología de la Organización de Estados de Seguridad...  
**1.1 NIVEL DE MADUREZ**  
Los criterios de la observación de seguridad se evalúan mediante un nivel de madurez...  
**ESQUEMA NACIONAL DE SEGURIDAD**  
NIVEL OPERATIVO: 4.0



# INES – OUTPUT

3



Generado por ines@ccn-cert.cni.es el 10/05/2017 a las 16:35 h.  
 Rellenada al: 93,56% y actualizada al 10/02/2017  
 Los cálculos se calculados según describe la guía CCN-STIC-824 versión Octubre 2016.

CUADRO DE MANDOS 2016

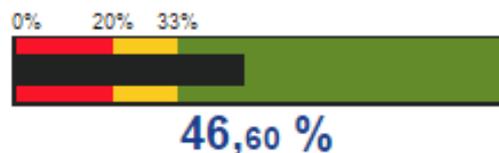


NOMBRE DEL ORGANISMO:  
 TIPO DEL ORGANISMO: AGE  
 COMUNIDAD AUTÓNOMA: No aplica

CATEGORÍA DE LOS SISTEMAS DE INFORMACIÓN: Básica  
 VALOR MÁXIMO DE LA DISPONIBILIDAD: Bajo  
 VALOR MÁXIMO DE LA INTEGRIDAD: Baja

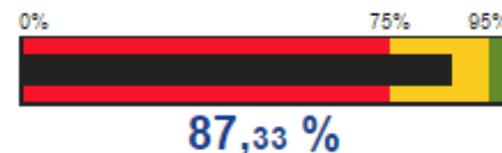
VALOR MÁXIMO DE LA CONFIDENCIALIDAD: Baja  
 VALOR MÁXIMO DE LA AUTENTICIDAD: Baja  
 VALOR MÁXIMO DE LA TRAZABILIDAD: Bajo

## INDICADOR DE MADUREZ DEL ENS (index.maturity.ens)



Mediana para AGE con sistemas de categoría Básica: 42,73 %  
 Mediana para AGE: 56,00 %  
 Pulse aquí para ver la información necesaria para calcular este indicador

## INDICADOR DE CUMPLIMIENTO DEL ENS (index.compliance.ens)



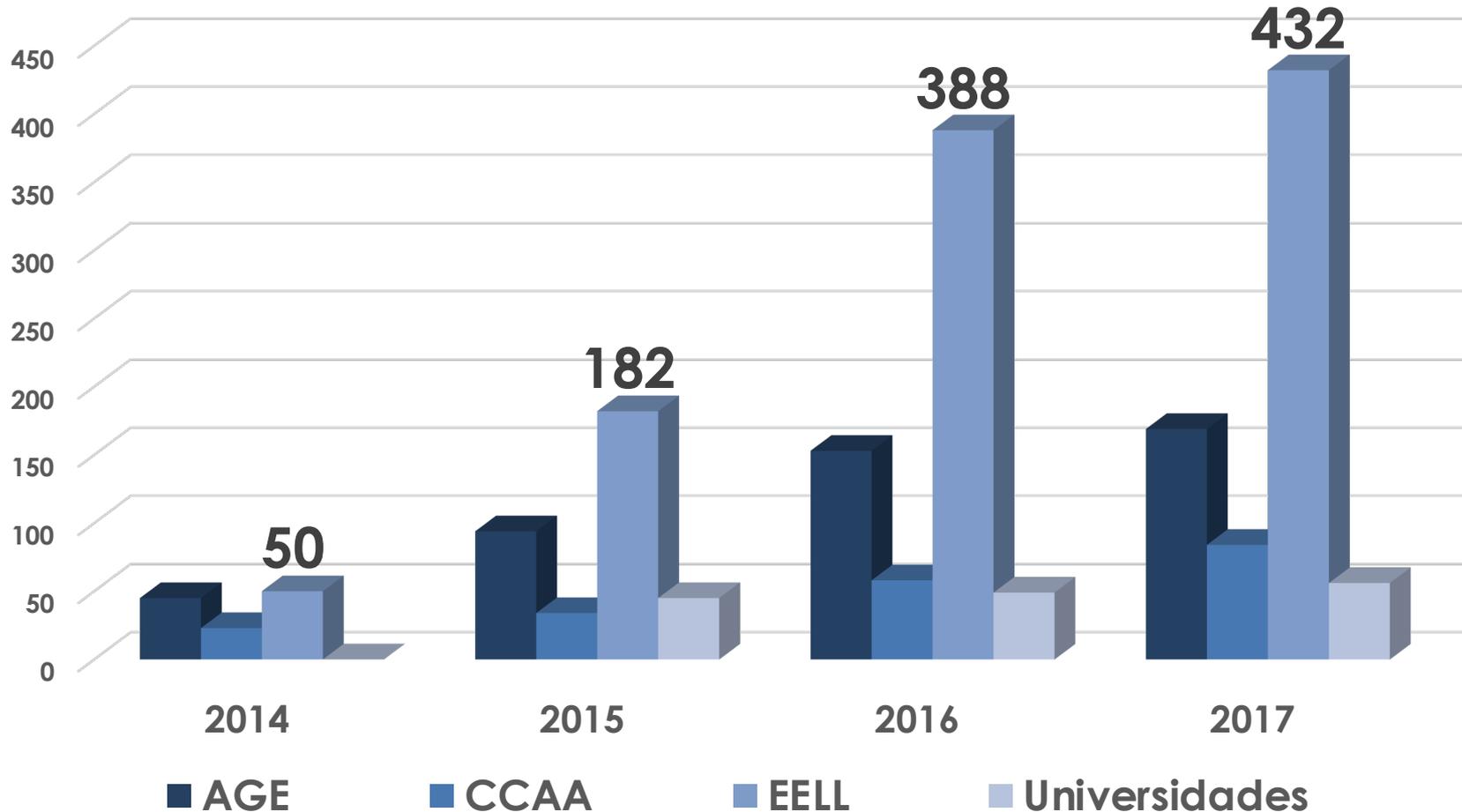
Mediana para AGE con sistemas de categoría Básica: 57,07 %  
 Mediana para AGE: 70,24 %  
 Pulse aquí para ver la información necesaria para calcular este indicador



# ÍNDICE

1. Herramienta INES
2. Participación (2017)
3. Categorización de Sistemas
4. Resultados
5. Conclusiones y próximos pasos

# EVOLUCIÓN DE PARTICIPACIÓN

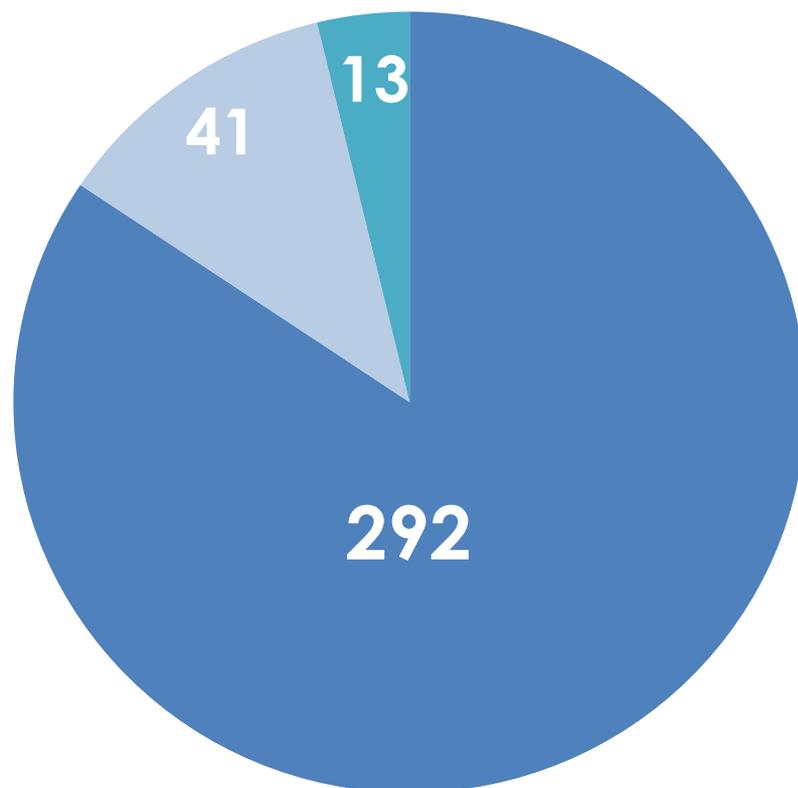


Hay un incremento del **11%** en volumen de fichas de las Entidades Locales

## DISTRIBUCIÓN POR TIPO DE ORGANISMO



Fichas creadas en INES:

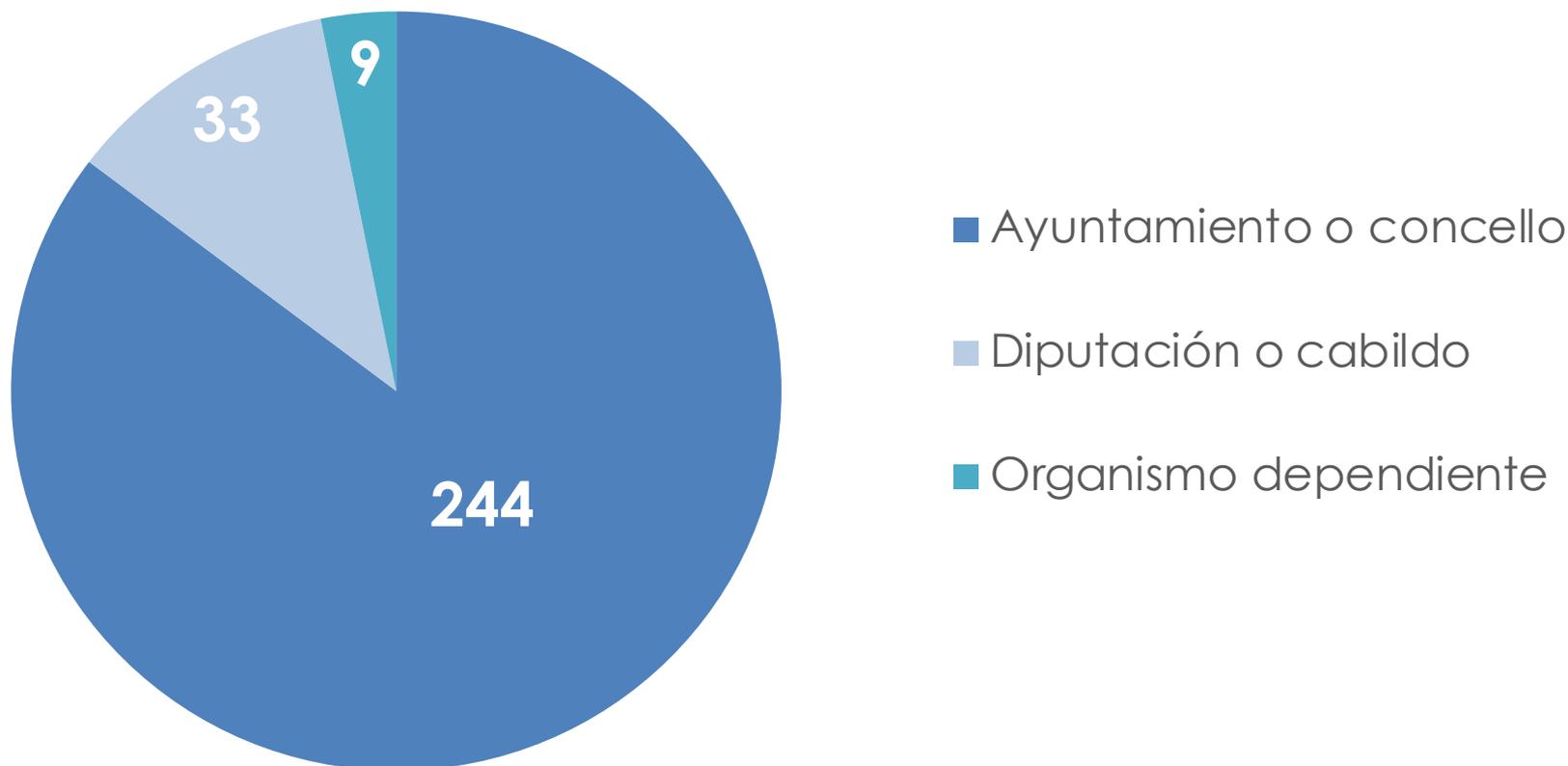


- Ayuntamiento o concello
- Diputación o cabildo
- Organismo dependiente

## DISTRIBUCIÓN POR TIPO DE ORGANISMO

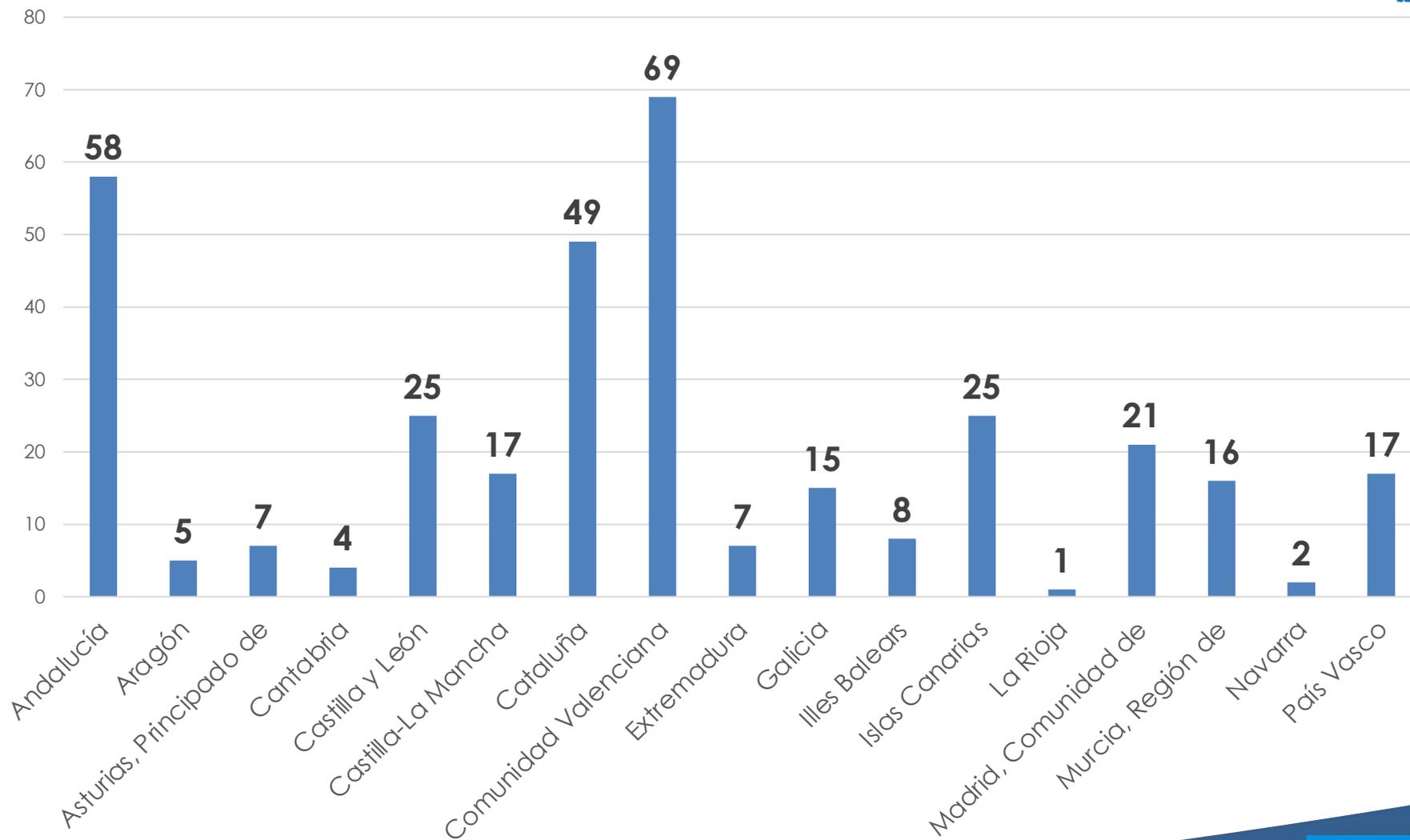


Fichas creadas en INES con más de un 50% de rellenado:



Estas fichas son las que se tendrían en cuenta en los informes globales

# DISTRIBUCIÓN POR COMUNIDAD AUTÓNOMA

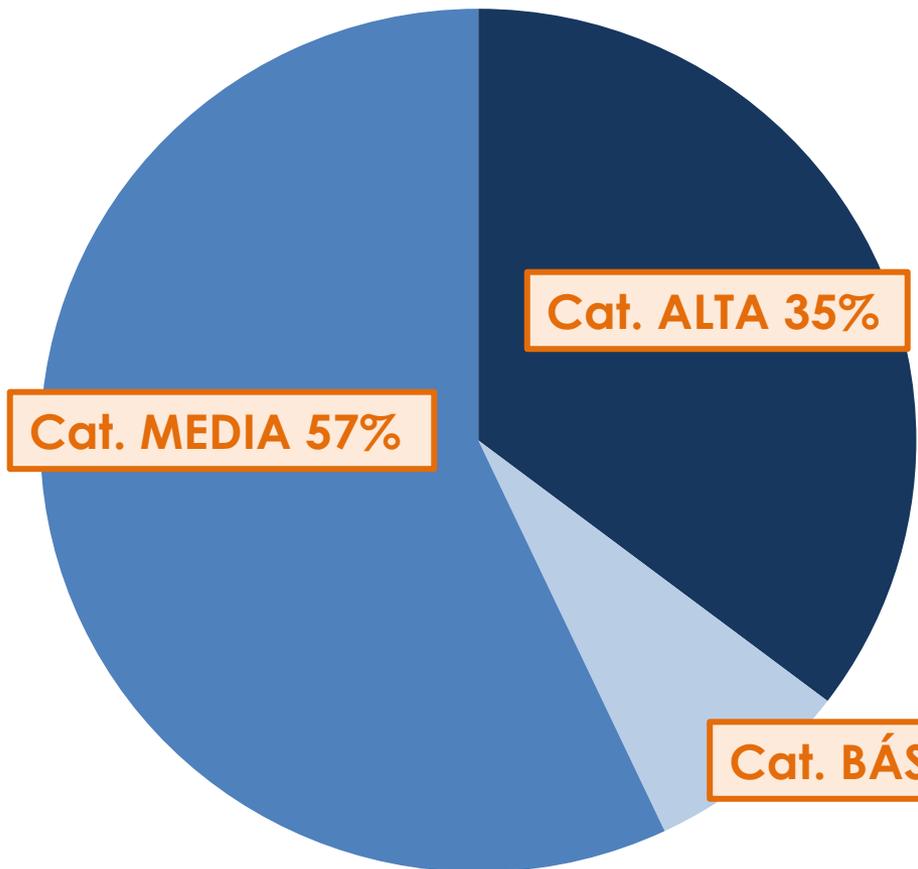




# ÍNDICE

1. Herramienta INES
2. Participación (2017)
3. Categorización de Sistemas
4. Resultados
5. Conclusiones y próximos pasos

# RESULTADOS INES 2016 – CATEGORÍAS



Ayuntamientos	BÁSICA	MEDIA	ALTA
< 20.000 hab.	4	19	6
De 20.001 a 75.000 hab.	9	59	49
≥ 75.000 hab.	2	41	27
Diputaciones y Cabildos	1	25	11



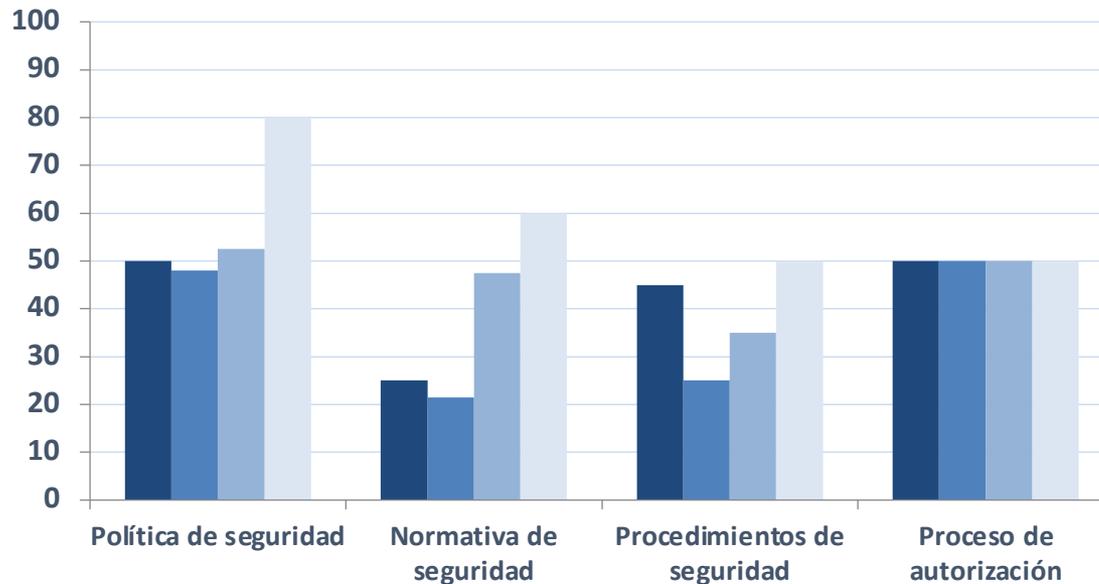
Consultar **CCN-STIC-803:Valoración de Sistemas**



# ÍNDICE

1. Herramienta INES
2. Participación (2017)
3. Categorización de Sistemas
4. Resultados
5. Conclusiones y próximos pasos

## RESULTADOS INES 2016 – ASPECTOS GENERALES



- Ayuntamientos de menos de 20.000 hab.
- Ayuntamientos de 20.001 a 75.000 hab.
- Ayuntamientos de más de 75.000 hab.
- Diputaciones y Cabildos

Elementos evaluados	AGE	CC.AA.	EE.LL.	UNIV.	Global
Política de Seguridad Aprobada	5	5	3	5	4
Independencia entre Responsables	4	5	3	5	4
Análisis de Riesgos	3	3	2	3	2
Declaración de Aplicabilidad	3	3	2	3	3
Plan de Adecuación	3	3	3	4	3
Certificación de cumplimiento	1	2	1	1	1

## RESULTADOS INES 2016 – RESULTADOS MEDIDAS ANEXO II



# ESQUEMA NACIONAL DE SEGURIDAD

## 75 MEDIDAS DE SEGURIDAD

### MARCO ORGANIZATIVO

El marco organizativo está constituido por un conjunto de medidas relacionadas con la organización global de la seguridad

4

POLÍTICA DE SEGURIDAD  
NORMATIVA DE SEGURIDAD  
PROCEDIMIENTOS DE SEGURIDAD  
PROCESO DE AUTORIZACIÓN

### MARCO OPERACIONAL

El marco operacional está constituido por las medidas a tomar para proteger la operación del sistema como conjunto integral de componentes para un fin

31

PLANIFICACIÓN  
CONTROL DE ACCESO  
EXPLOTACIÓN  
SERVICIOS EXTERNOS  
CONTINUIDAD DEL SERVICIO  
MONITORIZACIÓN DEL SISTEMA

### MEDIDAS DE PROTECCIÓN

Las medidas de protección, se centrarán en proteger activos concretos, según su naturaleza, con el nivel requerido en cada dimensión de seguridad.

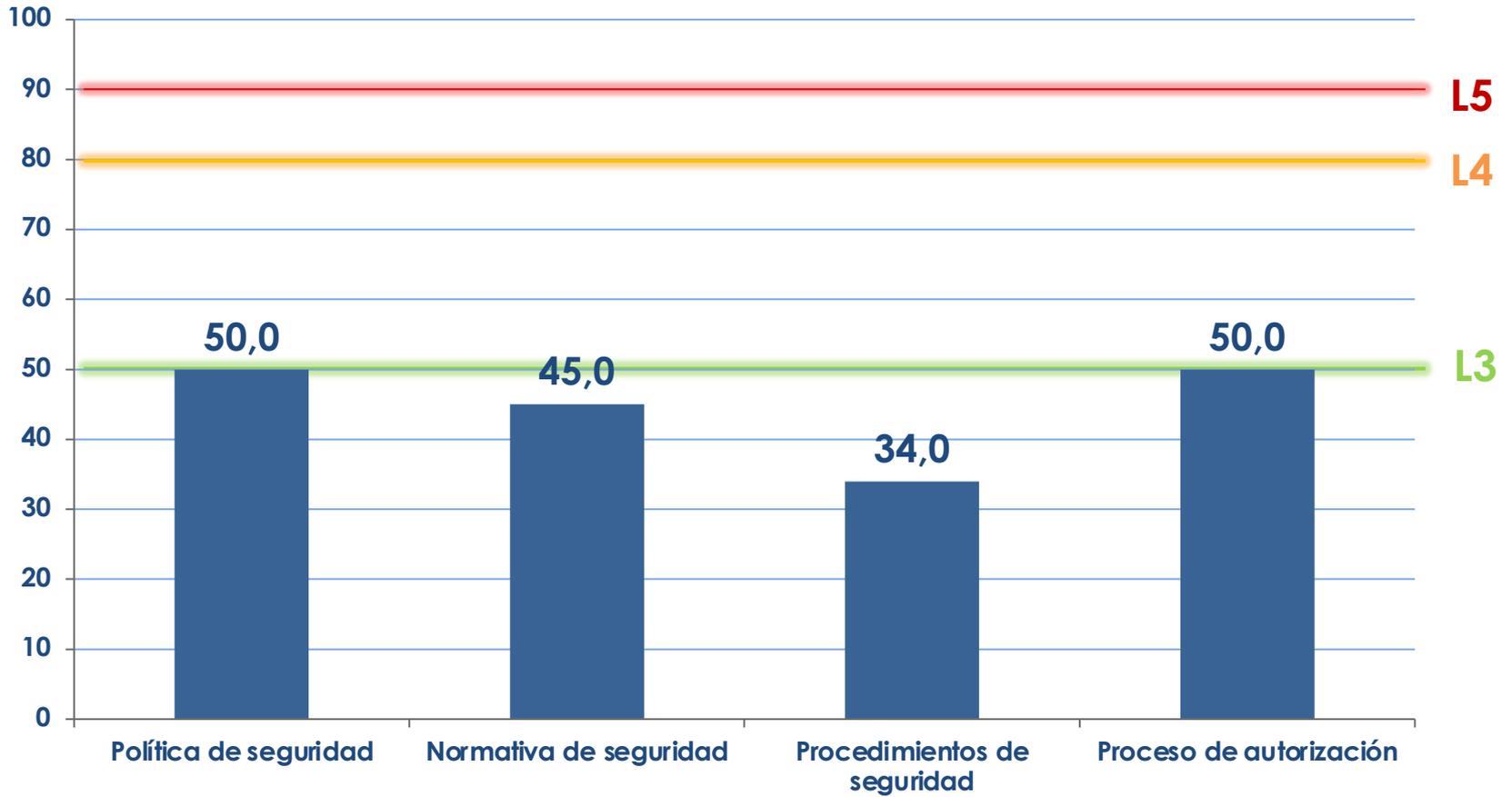
40

INSTALACIONES E INFRAESTRUCTURAS  
GESTIÓN DEL PERSONAL  
PROTECCIÓN DE LOS EQUIPOS  
PROTECCIÓN DE LAS COMUNICACIONES  
PROTECCIÓN SOPORTES DE INFORMACIÓN  
PROTECCIÓN APLICACIONES INFORMÁTICAS  
PROTECCIÓN DE LA INFORMACION  
PROTECCIÓN DE LOS SERVICIOS

Los resultados abarcan **6.182 sistemas TIC** que dan servicio a **232.790 usuarios**.

# RESULTADOS INES 2016 – RESULTADOS MEDIDAS ANEXO II

## Marco Organizativo



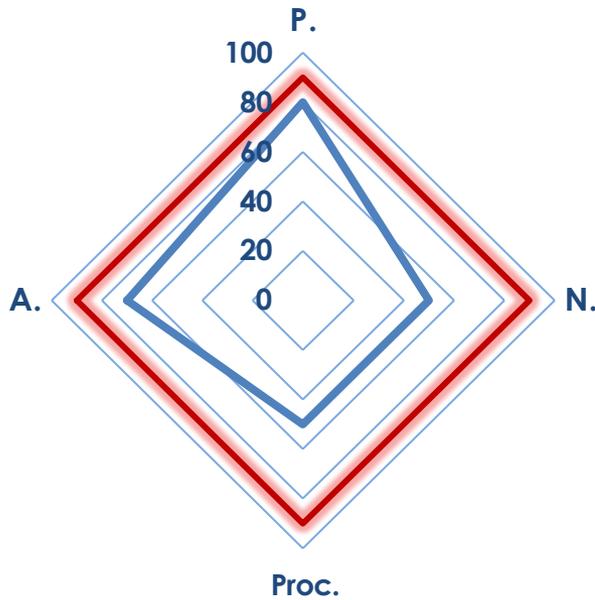
# RESULTADOS INES 2016 – RESULTADOS MEDIDAS ANEXO II

## Marco Organizativo

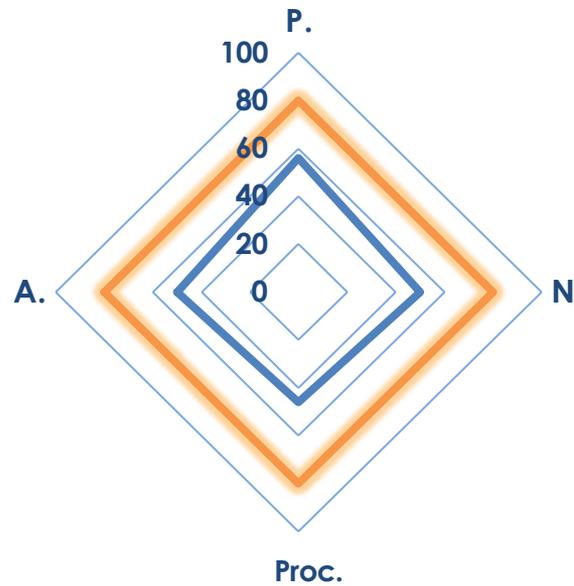
**Categoría Alta**

**Categoría Media**

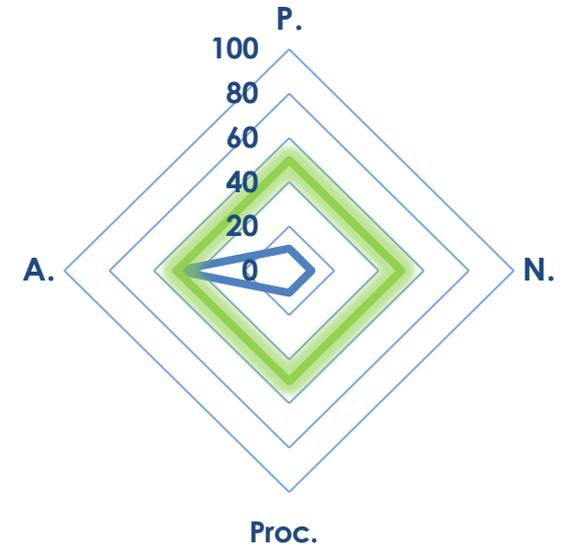
**Categoría Básica**



**P:** Política de Seguridad  
**N:** Normativa de Seguridad

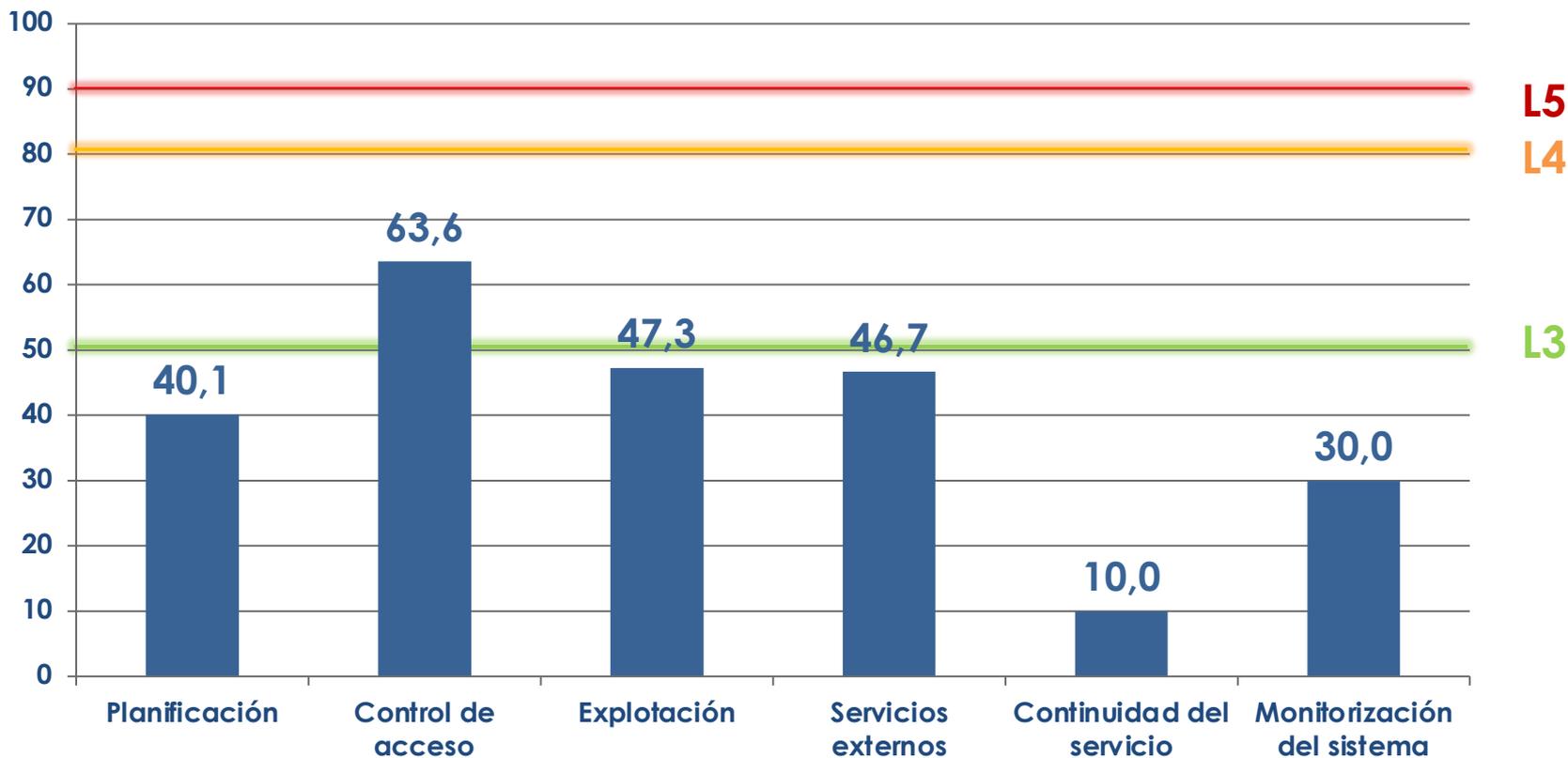


**Proc:** Procedimientos de Seguridad  
**A:** Proceso de autorización



# RESULTADOS INES 2016 – RESULTADOS MEDIDAS ANEXO II

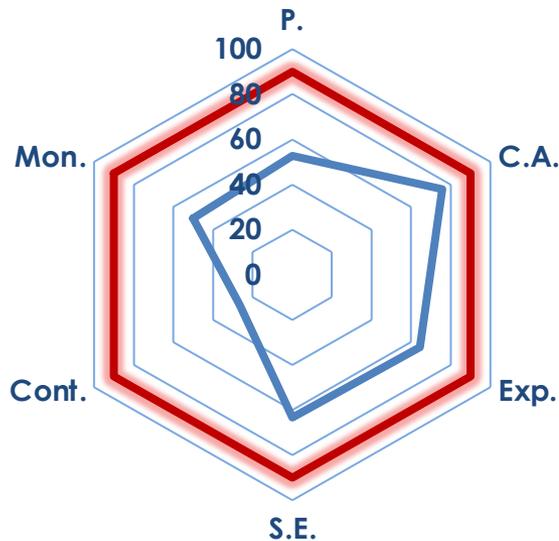
## Marco Operacional



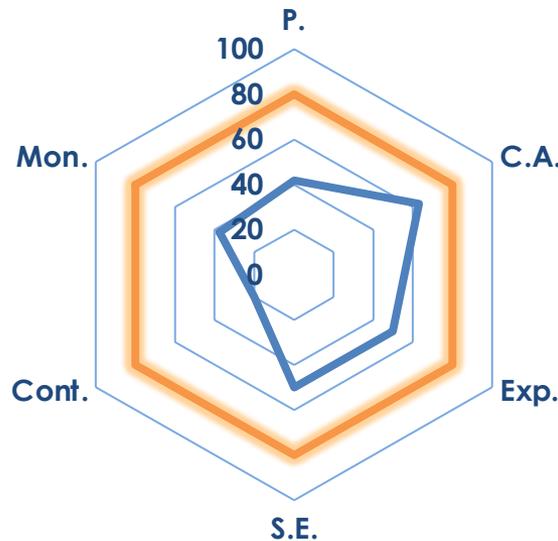
# RESULTADOS INES 2016 – RESULTADOS MEDIDAS ANEXO II

## Marco Operacional

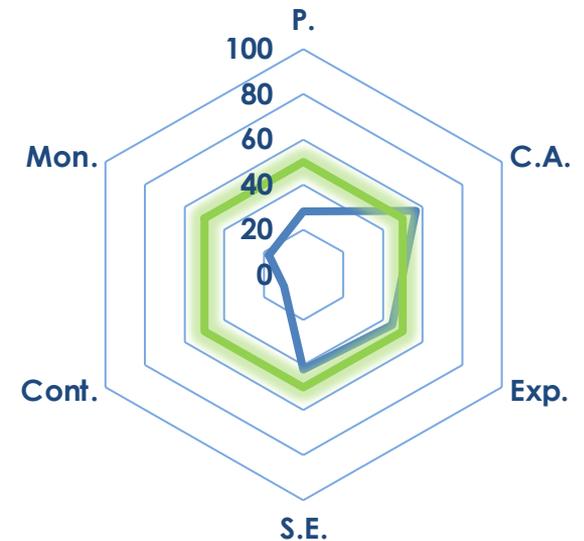
### Categoría Alta



### Categoría Media



### Categoría Básica

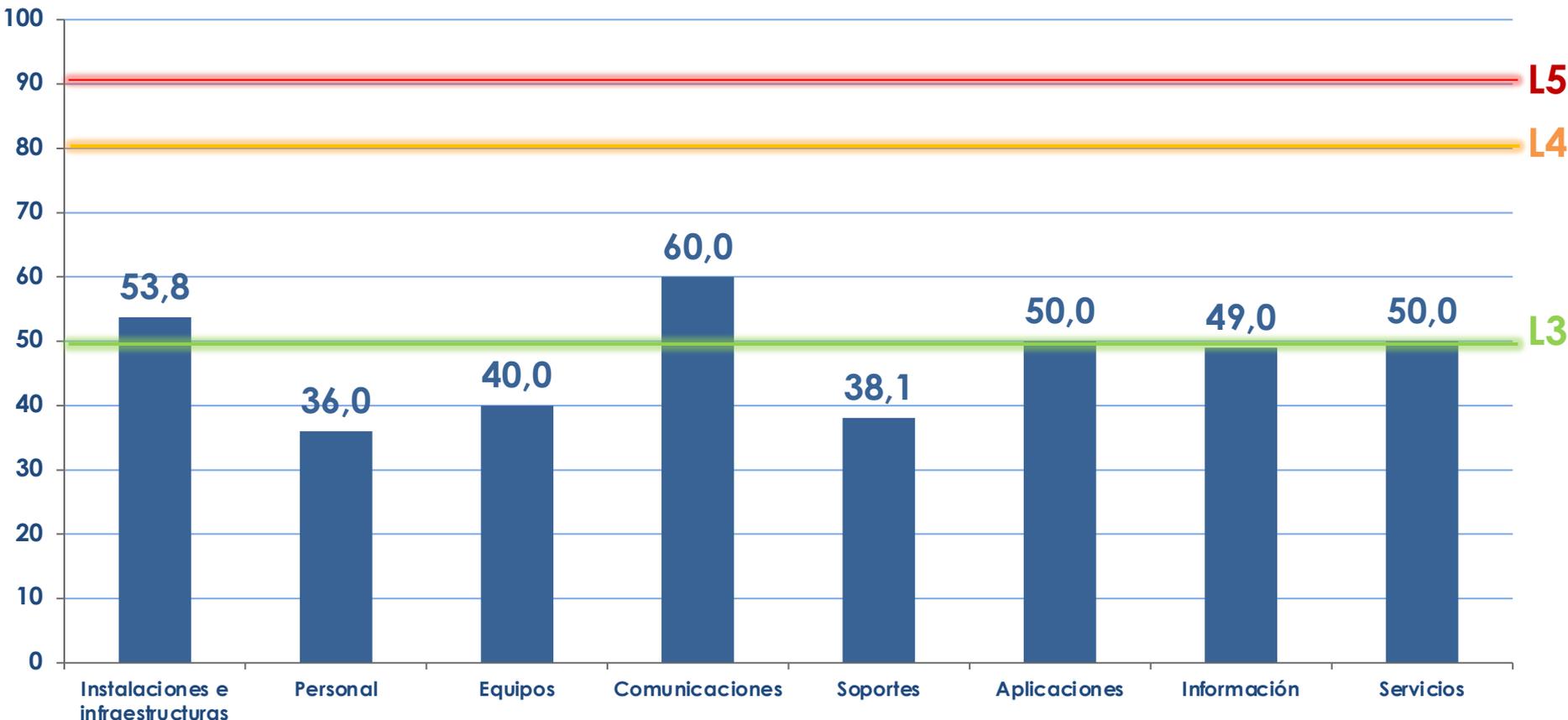


**P:** Planificación  
**C.A:** Control de accesos  
**Exp.:** Explotación

**S.E:** Servicio Externalizados  
**Cont:** Continuidad de servicio  
**Mon:** Monitorización

# RESULTADOS INES 2016 – RESULTADOS MEDIDAS ANEXO II

## Medidas de Protección



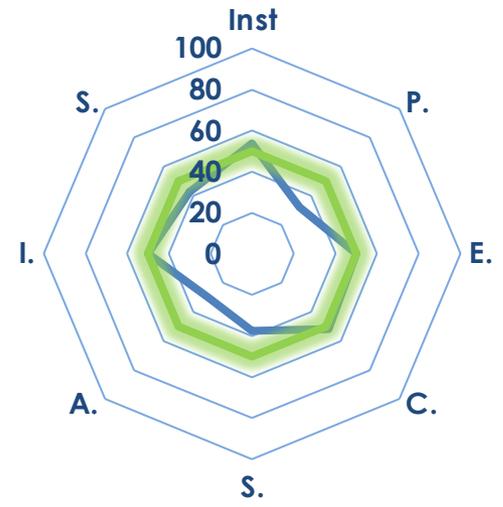
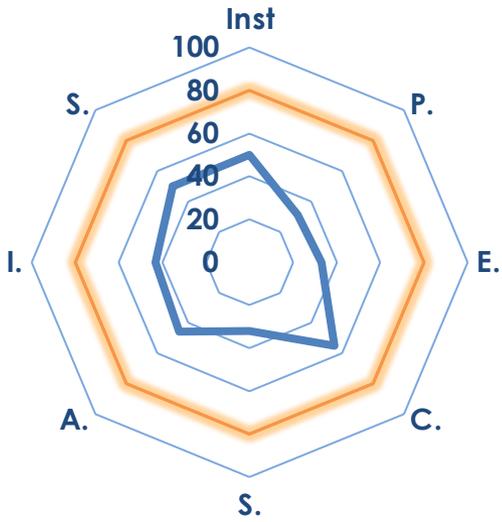
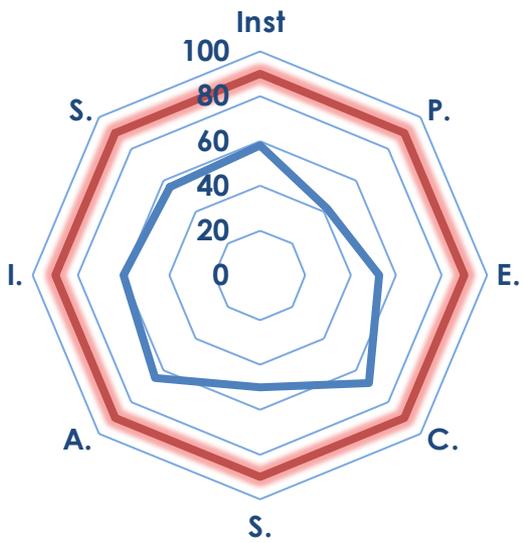
RESULTADOS INES 2016 – RESULTADOS MEDIDAS ANEXO II

Medidas de Protección

Categoría Alta

Categoría Media

Categoría Básica



Inst: Instalaciones e Infraestructuras  
 P: Personal

E: Equipos:  
 C: Comunicaciones  
 S: Soportes

A: Aplicaciones  
 I: Información  
 S: Servicios

## RESULTADOS INES 2016 – MEDIDAS INDIVIDUALES ANEXO II

	AGE	CCAA	EELL	UNIV.
[op.acc.1] Identificación	80	90	80	80
[op.acc.2] Requisitos de acceso	80	90	80	78
[op.acc.4] Proceso de gestión de derechos	75	80	75	63
[op.exp.6] Protección frente a código dañino	80	83	77	72
[mp.if.4] Energía eléctrica	90	90	80	90
[mp.if.5] Protección frente a incendios	90	90	80	90
[mp.com.1] Perímetro seguro	80	90	80	80
[mp.info.9] Copias de seguridad	88	90	80	90



	AGE	CCAA	EELL	UNIV.
[op.cont.1] Análisis de impacto	30	40	10	10
[op.cont.2] Plan de continuidad	15	50	10	12
[op.cont.3] Pruebas periódicas	10	50	10	5
[op.mon.2] Sistema de métricas	13	40	10	10
[mp.per.4] Formación	42	50	18	38
[mp.per.9] Personal alternativo	50	50	10	0
[mp.info.3] Cifrado de la información	50	50	10	25
[mp.info.6] Limpieza de documentos	20	10	10	10



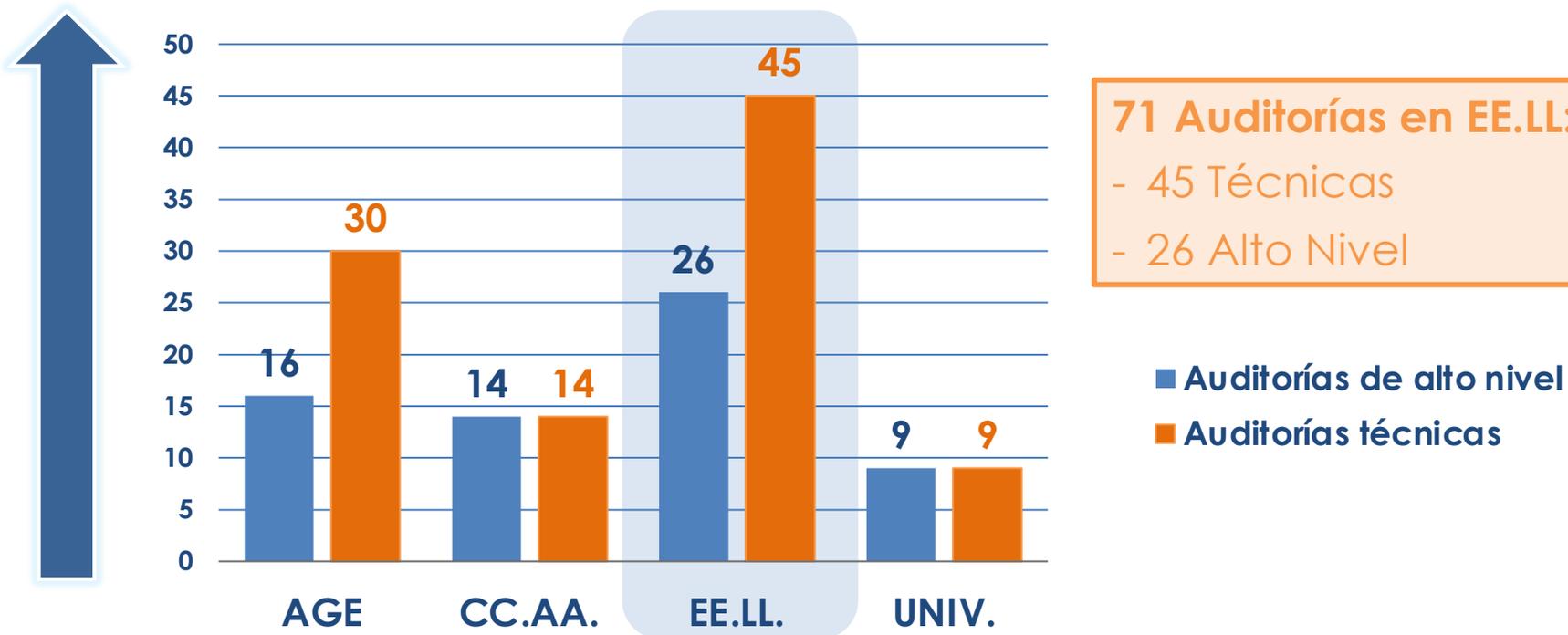
## RESULTADOS INES 2016 – PROCESOS CRÍTICOS

CCN-STIC 824

Procesos críticos	AGE	CC.AA.	EE.LL.	UNIV.	EE.LL. 2015
Proceso de Autorización (org.4)	50	80	50	42,5	49
Análisis de Riesgos (op.pl.1)	50	80	50	50	40
Gestión de derechos de acceso (op.acc.4)	75	80	75	52	70
Incidentes (op.ext.7)	62	80	50	67	50
Concienciación	50	61,8	35,8	45	10
Gestión de la configuración (op.exp.2 +op.exp.3)	60	70	50	50	25
Mantenimiento y Gestión de cambios (op.exp.4+op.exp.5)	58	79	50	50	25
Continuidad de operaciones (op.cont.1/2/3 y medios alternativos.9)	50	54	34,7	33,7	1

- A nivel comparativo, los procesos en los que las EE.LL han registrado valores más deficientes son la **Concienciación** y la **Gestión de Incidentes**.
- La situación de la **continuidad** es deficiente en todos los colectivos, especialmente en las Entidades Locales aunque con una **mejora elevada respecto a 2015**.
- Es todavía mejorable la **concienciación y formación** aunque con una **importante subida respecto a 2015**.
- Aunque hay procesos críticos cuyos indicadores en 2016 todavía no alcanzan los valores exigidos. En general, los indicadores **han mejorado respecto a los correspondientes de 2015**.

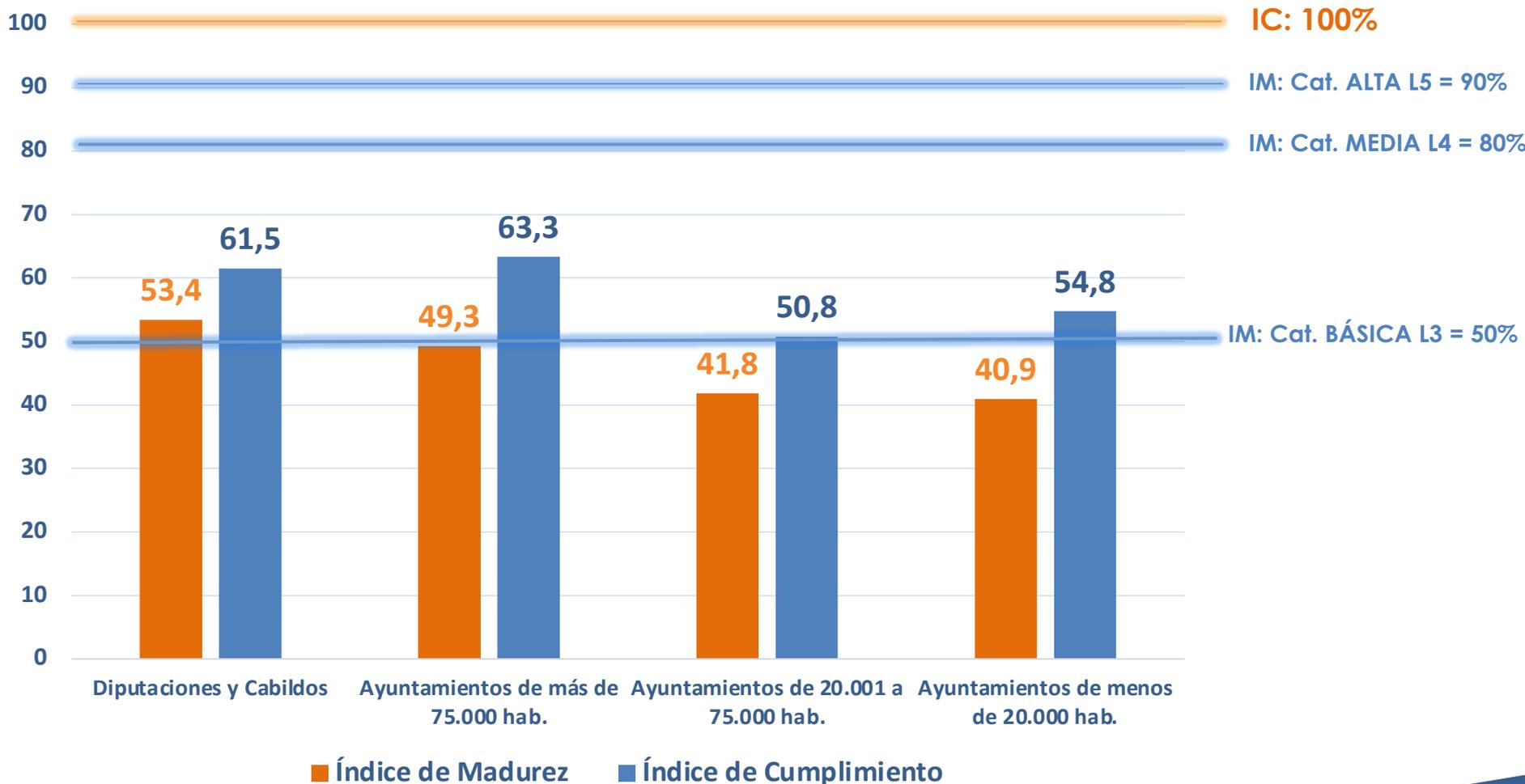
## RESULTADOS INES 2016 – AUDITORÍAS



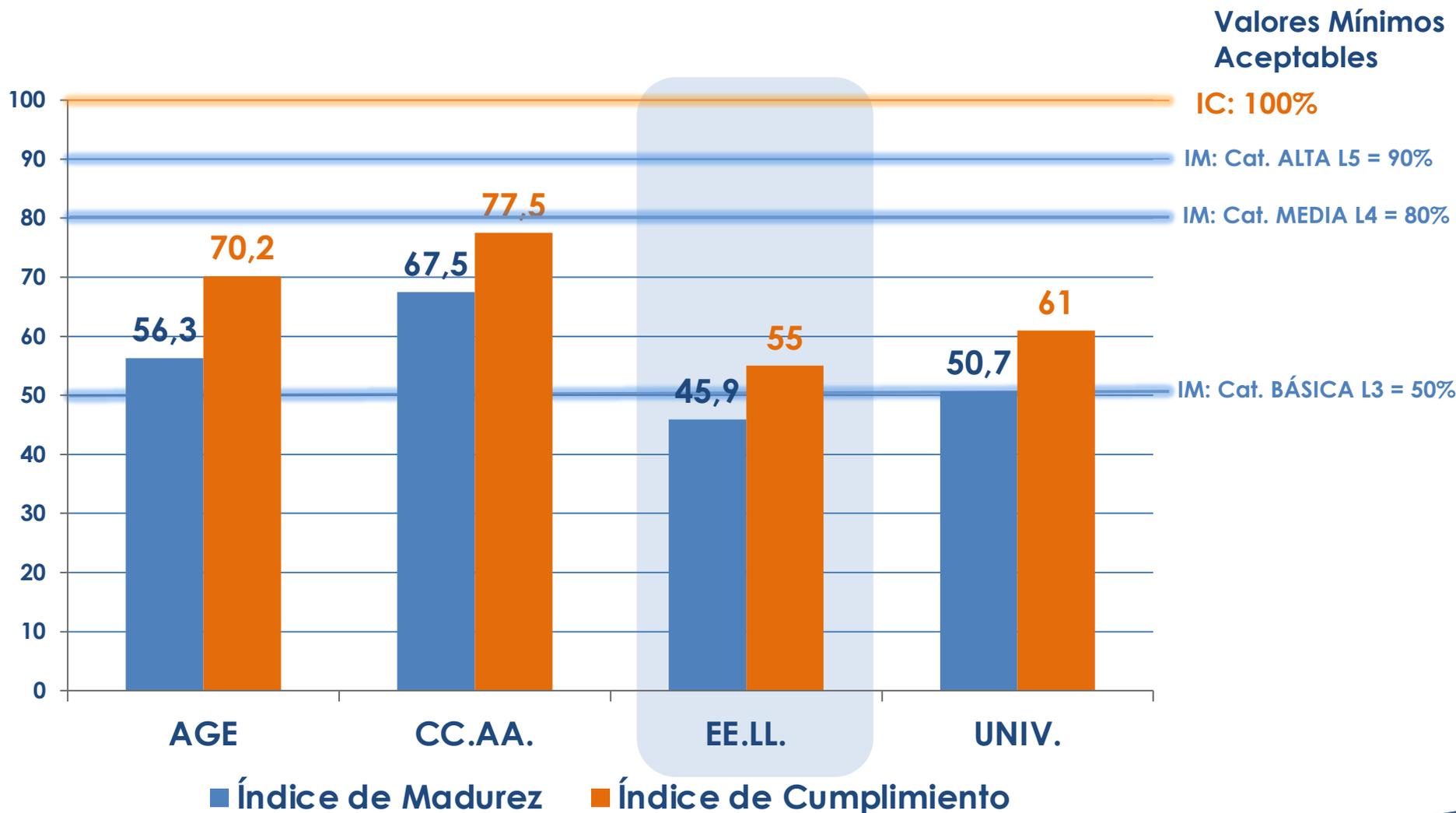
- Hay **8 ayuntamientos** que han declarado tener una **certificación de conformidad con el ENS**.
- Hay **202 EE.LL** que **no han realizado auditorías**, ni técnicas ni de alto nivel.
- El número de **auditorías en las EE.LL. ha aumentado un 30%** respecto a 2015 pero siguen siendo insuficientes.

# RESULTADOS INES 2016 – NIVEL DE MADUREZ/CUMPLIMIENTO

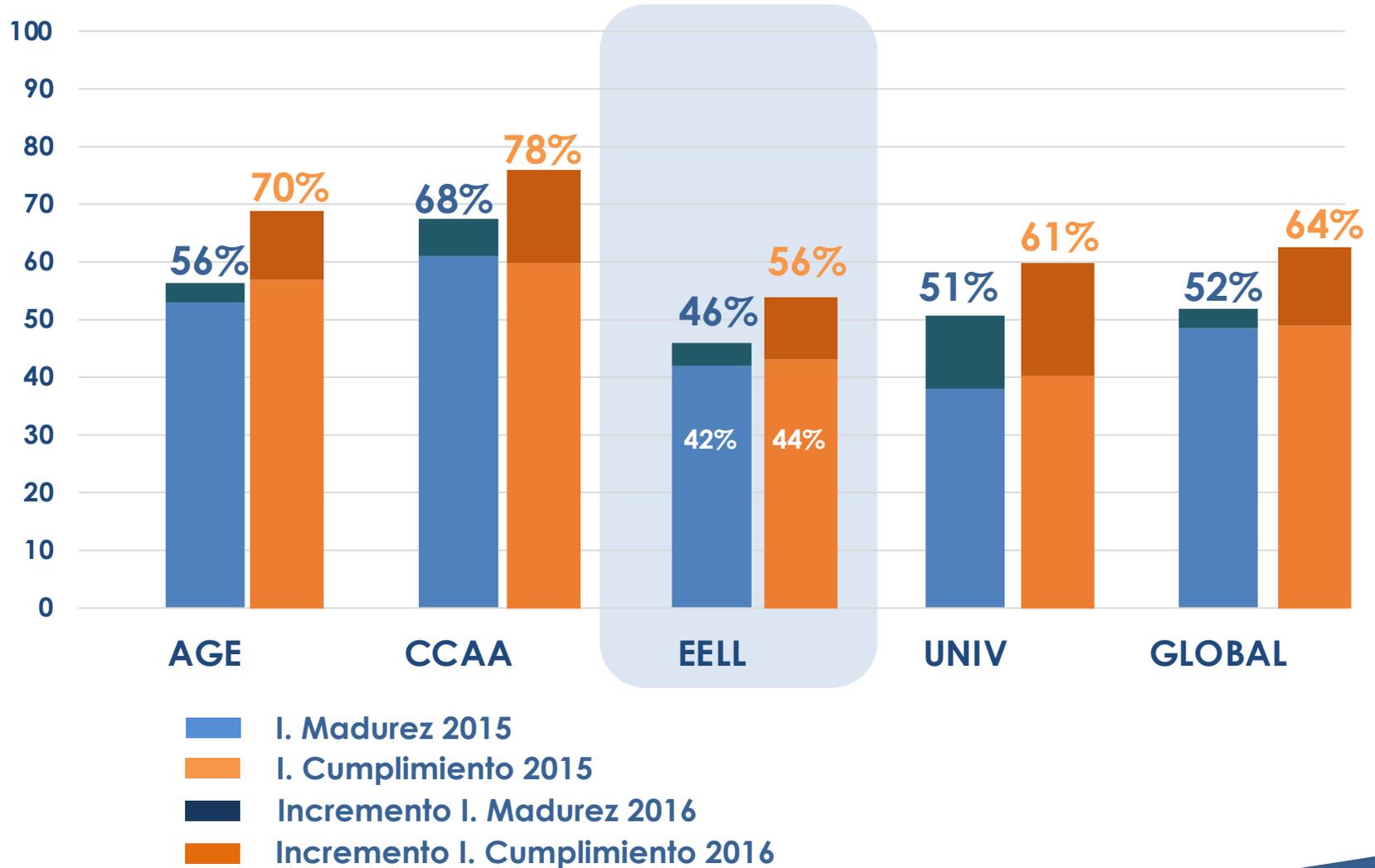
Valores Mínimos Aceptables



## RESULTADOS INES 2016 – NIVEL DE MADUREZ/CUMPLIMIENTO



# RESULTADOS INES 2016 – EVOLUCIÓN



# RESULTADOS INES 2016 – INFORMES

## RESULTADOS GENERALES

USO OFICIAL

**INFORME EJECUTIVO CCN-CERT IT 05/17  
RESULTADOS GENERALES**

**INFORME NACIONAL DEL ESTADO DE SEGURIDAD DE LOS SISTEMAS  
DE LAS TECNOLOGÍAS DE LA INFORMACIÓN Y LA COMUNICACIÓN**

Abril 2017

## RESULTADOS SECTORIALES

USO OFICIAL

**INFORME EJECUTIVO CCN-CERT IT 08/17  
RESULTADOS  
ENTIDADES LOCALES**

**INFORME NACIONAL DEL ESTADO DE SEGURIDAD DE LOS SISTEMAS  
DE LAS TECNOLOGÍAS DE LA INFORMACIÓN Y LA COMUNICACIÓN**

Abril 2017



# ÍNDICE

1. Herramienta INES
2. Participación (2017)
3. Categorización de Sistemas
4. Resultados
5. Conclusiones y próximos pasos

## RESULTADOS INES 2016 – CONCLUSIONES

- 1. Nivel de cumplimiento 2016 en las EE.LL. es BAJO (56%).** Retraso en la implementación.
- 2. Las EE.LL. tienen mucho recorrido pendiente en el proceso de adecuación al ENS,** siendo la certificación del cumplimiento del ENS el aspecto más significativo al respecto.
- 3. Es necesario mejorar algunos indicadores:**
  - Concienciación y Formación
  - Recursos
  - Mecanismos de Continuidad
- 4. Responsable de seguridad no es suficiente.**
  - Necesidad de equipos de seguridad
- 5. Pocas tareas de vigilancia de la red.**
  - No revisión de logs / No hay monitorización real.

## RESULTADOS INES 2016 – PRÓXIMOS PASOS

- Promover la **conformidad** con el ENS. En particular, fomentar la certificación a través de la realización de **auditorías independientes**. Necesidad de ajustar la **subjetividad**.
- Impulsar **medidas de seguridad horizontales** a toda la Administración en relación a la configuración de seguridad, gestión de incidentes y protección del correo electrónico, servicios y aplicaciones web.
- Promover plataformas de **Servicios en NUBE**:
  - Servicios de continuidad, monitorización y registro de actividad.
  - Plataforma de concienciación y formación basados en los servicios actuales del CCN.
- Obtener un **mayor compromiso** de los organismos.
- Impulsar la aprobación de las **Instrucciones Técnicas de Seguridad (ITS)** pendientes de publicar.

